(19)日本国特許庁（ＪＰ）　(12)公表特許公報（Ａ）　(11)特許出願公表番号
特表2002－542672
（P2002－542672A）
(43)公表日　平成14年12月10日(2002.12.10)

(51)Int.Cl.[7]		識別記号	FI		テーマコード(参考)	
H04L	9/08		G06F	12/14	320E	5B017
G06F	12/14	320		15/00	330A	5B035
	15/00	330	G09C	1/00	660G	5B085
G06K	19/00		H04L	9/00	601B	5J104
	19/07		G06K	19/00	N	

審査請求　未請求　予備審査請求　有　（全 26 頁）　最終頁に続く

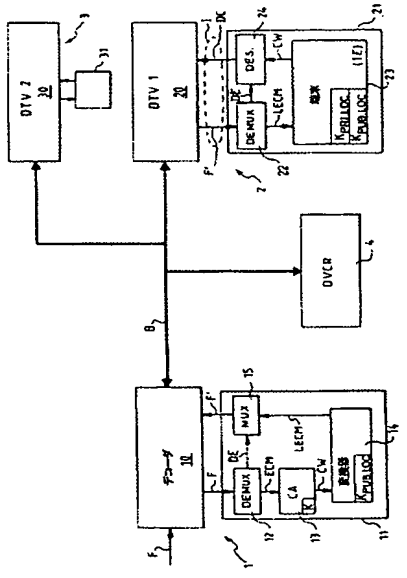
(21)出願番号　特願2000－611462(P2000－611462)
(86)(22)出願日　平成12年３月31日(2000.3.31)
(85)翻訳文提出日　平成13年10月10日(2001.10.10)
(86)国際出願番号　ＰＣＴ／ＥＰ００／０２９１８
(87)国際公開番号　ＷＯ００／６２５０５
(87)国際公開日　平成12年10月19日(2000.10.19)
(31)優先権主張番号　９９／０４７６７
(32)優先日　平成11年４月13日(1999.4.13)
(33)優先権主張国　フランス（ＦＲ）

(71)出願人　トムソン　ライセンシング　ソシエテ　アノニム
Ｔｈｏｍｓｏｎ　Ｌｉｃｅｎｓｉｎｇ　Ｓ．Ａ．
フランス国，　エフ－92100　ブローニュ　ビヤンクール，　ケ　アルフォンス　ルガロ，　46番地
(72)発明者　ケ，フロランス
フランス国，13006　マルセイユ，リュ・ド・ブルトゥイユ　169，レ・オー・ド・ブルトゥイユ　アパルトマン62　バティマン　アー
(74)代理人　弁理士　伊東　忠彦

最終頁に続く

(54)【発明の名称】　デジタルホームネットワークとデジタルホームネットワークの作成及び更新方法

(57)【要約】
ローカルデジタルネットワークは、ネットワークの外部から発するデータを受信し、そのデータをネットワークのあるポイントへ送信するアクセス装置（１）と、ネットワーク内を流れるデータを受信し、そのデータをネットワークのあるポイントで提示する提示装置（２，３）と、を有する。データは、ネットワーク内を暗号形式で流れ、ネットワークの全ての装置は、ネットワークにおけるデータの暗号化及び復号化用のローカル鍵である単一の鍵を使用する。好ましくは、ネットワークのローカル鍵は、公開鍵と秘密鍵のペアにより形成される。このネットワークの目的は、このローカルネットワーク内でのデータのコピーを許可し、他のネットワークを宛先とする不正コピーを禁止することである。



【特許請求の範囲】

【請求項１】　ネットワークの外部から発するデータを受信し、該ネットワークのあるポイントへ送信することができる少なくとも一台のアクセス装置（１）と、

ネットワークのあるポイントで提示すべく、ネットワークを流れるデータを受信するよう適応した少なくとも一台の提示装置（２，３）と、

を有し、

データは暗号形式だけで流れるように適応している、ローカルデジタルネットワーク、特に、デジタルホームネットワークであって、

該ネットワークの全ての装置は、ネットワークを流れるデータの暗号化及び復号化のため、ネットワークに特有の単一の暗号鍵であるネットワークのローカル鍵（$K_{PUB.LOC}$，$K_{PRI.LOC}$）を使用することを特徴とする、デジタルネットワーク。

【請求項２】　データは公開鍵暗号システムを用いて暗号化され、

ネットワークの該ローカル鍵は、公開鍵と秘密鍵のペアであるローカル公開鍵（$K_{PUB.LOC}$）及びローカル秘密鍵（$K_{PRI.LOC}$）により構成されることを特徴とする、請求項１記載のデジタルネットワーク。

【請求項３】　該ネットワークに接続された提示装置（２，３）だけがローカル秘密鍵（$K_{PRI.LOC}$）を保持することを特徴とする請求項２記載のデジタルネットワーク。

【請求項４】　所与の時点で、ネットワークの単一の提示装置は、ローカル秘密鍵（$K_{PRI.LOC}$）を、該ネットワークへ接続するよう適した新しい提示装置へ送信するよう許可されていることを特徴とする請求項３記載のデジタルネットワーク。

【請求項５】　所与の時点で、提示装置は、

ｉ）提示装置が最初にネットワークへ接続されたときのバージン状態（ＩＥ＝００）である第１の状態と、

ｉｉ）提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態（ＩＥ＝０１）

である第２の状態と、

ｉｉｉ）提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態（ＩＥ＝１０）である第３の状態と、

の三つの状態の中でただ一つの状態だけを取ることができ、

提示装置は、上位ランクの状態へ移る場合に限り状態を変更するよう適応している、

ことを特徴とする請求項３記載のデジタルネットワーク。

【請求項６】　ネットワークの単一の提示装置が、第２の状態、すなわち、ネットワークの親である親状態にあることを特徴とする請求項５記載のデジタルネットワーク。

【請求項７】　所与の時点で、ネットワークの親は、該ネットワークに最後に接続された提示装置であることを特徴とする請求項６記載のデジタルネットワーク。

【請求項８】　請求項２乃至７のうちいずれか一項記載のデジタルネットワークに接続するよう適応した提示装置であって、

所与の時点で、該提示装置は、

ｉ）提示装置が最初にネットワークへ接続されたときのバージン状態（ＩＥ＝００）である第１の状態と、

ｉｉ）提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態（ＩＥ＝０１）である第２の状態と、

ｉｉｉ）提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態（ＩＥ＝１０）である第３の状態と、

の三つの状態の中でただ一つの状態だけを取ることができ、

提示装置は、上位ランクの状態へ移る場合に限り状態を変更するよう適応している、

ことを特徴とする提示装置。

【請求項９】　該提示装置がバージン状態にあるとき、該提示装置は、固有の公開鍵と秘密鍵のペアを保持し、接続されるのに適したネットワークのローカル鍵のペアを受信することが許可され、固有の鍵のペアの代わりに受信したローカル鍵のペアを保持することを特徴とする、請求項８記載の提示装置。

【請求項１０】　該提示装置が無効状態にあるとき、該提示装置は、接続されるネットワークのローカル鍵のペアを受信することが許可されなくなる、請求項８又は９記載の提示装置。

【請求項１１】　該提示装置は、該提示装置が占める状態を保持する記憶手段を有し、この記憶手段はスマートカードに統合されている、ことを特徴とする請求項８乃至１０のうちいずれか一項記載の提示装置。

【請求項１２】　ネットワークのローカル鍵のペアは、上記提示装置に装備されたスマートカード内に収容されていることを特徴とする、請求項８乃至１１のうちいずれか一項記載の提示装置。

【請求項１３】　請求項5.乃至７のうちいずれか一項記載のローカルデジタルネットワークを作成する方法であって、

デジタルバス（Ｂ）を介して、アクセス装置（１）と、公開鍵（K_{PUB_2}）及び秘密鍵（K_{PRI_2}）のペアを収容するバージン状態の提示装置（２）とを接続するステップ（ａ）と、

提示装置（２）において、該バス（Ｂ）を介して公開鍵（K_{PUB_2}）を配布するステップ（ｂ）と、

アクセス装置（１）において、該公開鍵（K_{PUB_2}）を受信し、公開鍵をネットワークの新しいローカル鍵（$K_{PUB.LOC}=K_{PUB_2}$）として保持し、該バスを介して、提示装置の状態変更信号を配布するステップ（ｃ）と、

提示装置（２）において、該状態変更信号を受信し、親状態（ＩＥ＝０１）へ移るステップ（ｄ）と、

を有することを特徴とする方法。

【請求項１４】　バージン状態（ＩＥ＝００）にあり、公開鍵（K_{PUB_3}）及び秘密鍵（K_{PRI_3}）を保持する新しい提示装置（３）を、請求項５乃至７のうちいずれか一項記載のローカルデジタルネットワークへ接続する方法であ

って、

新しい提示装置（３）をデジタルバス（Ｂ）を用いて該ローカルネットワークへ接続するステップ（ｅ）と、

新しい提示装置（３）において、該バス（Ｂ）を介して、公開鍵（K_{PUB3}）を配布するステップ（ｆ）と、

該ネットワークの少なくとも一台のアクセス装置（１）において、新しい提示装置の公開鍵（K_{PUB3}）を受信し、該アクセス装置が既にネットワークの公開鍵であるローカル公開鍵（$K_{PUB.Loc}$）を保持しているかどうかを照合し、保持している場合に、該バス（Ｂ）を介して、ネットワークのローカル公開鍵を配布するステップ（ｇ）と、

新しい提示装置（３）において、ネットワークのローカル公開鍵（$K_{Pub.Loc}$）を受信し、ローカル公開鍵を記憶し、該バスを介して、ネットワークの全ての提示装置を宛先として、親状態の提示装置からの応答を要求する応答要求信号を配布するステップ（ｈ）と、

ネットワークの親提示装置（２）において、応答要求信号を受信し、無効状態（ＩＥ＝１０）へ移り、新しい提示装置（３）に応答して、ネットワークローカル秘密鍵（$K_{PRI.Loc}$）を、新しい提示装置（３）が復号化可能な暗号形式で配布するステップ（ｉ）と、

新しい提示装置（３）において、ネットワークの該ローカル秘密鍵（$K_{PRI.Loc}$）を受信し、該ローカル秘密鍵を記憶し、受信承認信号を、ネットワークの前の親提示装置である提示装置（２）へ配布するステップ（ｊ）と、

ネットワークの前の親提示装置である提示装置（２）において、該受信承認信号を受信し、状態変更信号を新しい提示装置（３）へ配布するステップ（ｋ）と、

新しい提示装置（３）において、該状態変更信号を受信し、親状態（ＩＥ＝０１）へ移るステップ（ｌ）と、

を有する、方法。

【発明の詳細な説明】

【０００１】

本発明は、一般的に、ローカルデジタルネットワークの分野に係り、特に、デジタルホームネットワークの分野に関する。

【０００２】

このようなネットワークは、たとえば、IEEE　1394標準に準拠したバスのようなデジタルバスによって相互連結された装置の組により構成される。ネットワークは、２種類の装置、すなわち、

ローカルネットワークの外部から発したデータを受信し、ネットワークの接続されたあるポイントへそのデータを送信することができるアクセス装置と、

ネットワーク内を流れるデータをネットワークの接続された別のポイントへ提示するため、ネットワーク内を流れるデータを受信するよう適合した提示装置と、

を有する。第２のタイプの装置は、ローカルネットワークの外部とのリンクを具備していない。

【０００３】

オーディオ及び／又はビデオデータを住宅の種々の部屋へ伝達することを目的としたデジタルホームネットワークの一例を考えると、アクセス装置は、ネットワークの外部から、衛星アンテナ若しくはケーブルコネクションを介して、ビデオ番組を受信するデジタルデコーダ又はセットトップ・ボックス、或いは、光ディスクから読み出したデータ（オーディオ及び／又はビデオ）をデジタル形式でネットワーク上にブロードキャストする光ディスクの読取装置である（本例の場合に、ディスクはネットワークの外部から発したデータを収容する。）。提示装置は、たとえば、ネットワークから受信したビデオ番組を見ることができるテレビジョン受像機、或いは、より一般的には、受信したデジタル情報をエンドユーザへブロードキャストするため、受信したデジタル信号をアナログ形式に変換することができる装置である。

【０００４】

上述のタイプのホームネットワークは、ネットワークの外部とのリンクを具備

せず、ネットワーク内を流れるデータを記録する機能を有する第３のタイプの装置を含む。この第３のタイプの装置の一例として、特に、デジタルビデオレコーダ、又は、ＤＶＤ（デジタル汎用ディスク）タイプの光ディスクを記録することができる装置を挙げることができる。

【０００５】

全く同じ装置が、上述の二つ以上の異なる装置カテゴリーに属し得ることに注意する必要がある。たとえば、光ディスクを記録する装置は、商業的に予め記録されたディスクを読み取ることが可能であるため、上述の第１の装置のカテゴリーと第３の装置のカテゴリーに同時に属している。

【０００６】

ローカルネットワークの外部から発したデータを供給するコンテンツプロバイダ、特に、有料テレビ番組をブロードキャストするサービスプロバイダ、若しくは、たとえば、その他の光ディスクの発行元の立場を考えると、これらの伝送されたデータがコピーされること、及び、（たとえば、光ディスク若しくはその他の記録媒体へコピーされることによって）あるローカルネットワークから別のローカルネットワークへ容易に流出し得ることを防止する必要がある。

【０００７】

このため、実際には、鍵を使用する暗号化アルゴリズムを用いてデータを暗号化することにより、データを秘密形式で伝送することが知られている。この鍵は、これらのデータを受信することが許可されている装置に対し事前に公開されているか、或いは、コンテンツプロバイダとそれらの装置との間で特定の安全なプロトコルに従って交換される。

【０００８】

デジタルホームネットワークを保有するユーザの立場を考えると、これらのデータは、ネットワーク内の１台の装置がコンテンツプロバイダからデータを受信する権利を付与されているときには、ネットワークの他の全ての装置へ送信可能であることが望ましい。したがって、有料テレビサービスの加入者であり、かつ、（暗号形式で送信された）番組をラウンジに設置された（番組の復号化を許可された）セットトップ・ボックスで受信するユーザは、これらの番組を、たとえ

ば、寝室に設置されたテレビジョンで視聴できることを希望する。さらに、ユーザは、受信した番組を記録し、後で、たとえ、その有料テレビサービスの加入者ではなくなったときでも、ネットワークの数台の装置でその番組を視聴できることに関心がある。

【０００９】

コンテンツプロバイダの要望と、ユーザの要望とを考慮することにより、本発明は、ローカルデジタルネットワークで受信されたデータがネットワークの種々の装置の間で自由に流れ、そのデータがあるローカルネットワークから別のローカルネットワークへ流れることを阻止する手段の提供を目的とする。

【００１０】

この目的を達成するため、本発明が提案するローカルデジタルネットワーク、特に、デジタルホームネットワークは、

ネットワークの外部から発するデータを受信し、そのデータをネットワークのあるポイントへ送信することができる少なくとも一台のアクセス装置と、

データが暗号形式だけで流れるように適応したネットワーク内を流れるデータを受信するよう適応し、ネットワークのあるポイントでそのデータを提示する少なくとも一台の提示装置と、

を有する。本発明によれば、ネットワークの全ての装置は、ネットワークを流れるデータの暗号化及び復号化のため、ネットワークに特有の単一の暗号鍵、すなわち、ネットワークのローカル鍵を使用する。

【００１１】

各ローカルネットワークは、他のローカルネットワークのローカル鍵とは異なる固有のローカル鍵を保有するので、ローカルネットワークへ入った情報は、ネットワークの全ての装置が同じように読むことができるが、他のローカルネットワークで読むためにコピーすることはできない。より正確に表現すると、情報は、暗号形式でコピーすることができるが、その情報がコピーされたローカルネットワークとは異なる別のローカルネットワークにおいてその情報を再生できない。したがって、本発明は、コンテンツプロバイダの要望と、ユーザの要望の両方を満たす。

【００１２】

本発明の好ましい一局面によれば、データは、非対称暗号システムと呼ばれる、公開鍵による暗号システムを用いて暗号化される。ネットワークのローカル鍵は、本例の場合に、公開鍵と秘密鍵のペア、すなわち、ネットワークのローカル公開鍵とローカル秘密鍵とによって構成される。

【００１３】

好ましくは、ネットワークに接続された提示装置だけがローカル秘密鍵を知っている。

【００１４】

具体的な一実施例によれば、ある時点で、ネットワークの単一の提示装置は、ローカル秘密鍵を、ネットワークに接続するのに適した新しい提示装置へ送信することが許可される。この装置は、その後、ネットワークの「親」と呼ばれる。

【００１５】

ネットワークの「親」である装置が、特に、初期ローカルネットワークと同じローカル鍵を保有する不正ローカルネットワークを作成するため、ローカルネットワークから取り外されたとき、初期ローカルネットワークの装置は、ローカル秘密鍵を、初期ローカルネットワークに接続するため適した新しい提示装置へ送信し得なくなるので、初期ローカルネットワークは変更できなくなる。

【００１６】

本発明の他の局面によれば、所与の時点で、提示装置は、以下の状態の中でただ一つの状態だけを取ることができる。

【００１７】

ｉ）提示装置が最初にネットワークへ接続されたときのバージン状態である第１の状態。

【００１８】

ｉｉ）提示装置が、ネットワークのローカル秘密鍵を、ネットワークへ接続するのに適した新しい提示装置へ送信することが許可された親状態である第２の状態。

【００１９】

ｉｉｉ）提示装置は、ネットワークのローカル秘密鍵を、ネットワークへ接続する適性を備えた新しい提示装置へ送信することが許可されなくなる無効状態である第３の状態。

【００２０】

提示装置は、上位ランクの状態へ移る場合に限り、すなわち、バージン状態から親状態へ、或いは、親状態から無効状態へ移る場合に限り、状態を変更することができる。

【００２１】

本発明の好ましい一局面によれば、ネットワークの単一の提示装置は、第２の状態、すなわち、ネットワークの親である親状態にある。

【００２２】

具体的な一実施例によれば、所与の時点で、ネットワークの親は、ネットワークに最後に接続された提示装置である。

【００２３】

したがって、ネットワークの親の称号は、ローカルネットワークに接続された新しい提示装置へ渡される。これにより、単一の親提示装置から始めて、同じローカル鍵を有するローカルネットワークを順番に作成する不正行為を可能にさせることが阻止される。

【００２４】

また、本発明は、上述のように、デジタルネットワークに接続されるよう適応し、所与の時点で、上述のバージン状態、親状態又は無効状態の中のいずれか一つの状態だけを取ることができ、上位ランクの状態へ移るような状態の変更だけを行うように適応した提示装置に関する。

【００２５】

本発明の一局面によれば、提示装置がバージン状態にあるとき、提示装置は、固有の公開鍵と秘密鍵のペアを保有し、接続されるのに適したネットワークのローカル鍵のペアを受信することが許可され、固有の鍵のペアの代わりに受信したローカル鍵のペアを保持する。

【００２６】

本発明の他の局面によれば、提示装置が無効状態にあるとき、提示装置は、接続される適性のあるネットワークのローカル鍵のペアを受信することが許可されなくなる。

【００２７】

本発明の他の局面によれば、提示装置は、上記提示装置が占める状態を保持する手段を有し、この記憶手段はスマートカードに統合されている。

【００２８】

本発明の更に別の局面によれば、ネットワークのローカル鍵のペアは、上記提示装置に装備されたスマートカード内に収容されている。

【００２９】

また、本発明は、上述のネットワークのようなネットワークを作成し、更新する方法に関する。この方法については後述する。

【００３０】

本発明のその他の特徴及び利点は、添付図面と共に、以下の本発明の具体的、例示的な実施例の説明から明らかになるであろう。

【００３１】

添付図面を通じて、本発明と、以下に説明する本発明の具体的な実施例とを理解するために重要な要素だけが示されている。

【００３２】

アクセス装置１と、２台の提示装置２と、一般的にＤＶＣＲ（デジタルビデオカセットレコーダの略）と称されるデジタルビデオレコーダ４とを含むデジタルホームネットワークが図１に示されている。装置１、２、３及び４の組立体は、たとえば、ＩＥＥＥ１３９４標準に準拠した家庭用デジタルバスＢに接続される。

【００３３】

アクセス装置１は、スマートカード１１を装備したスマートカードリーダを具備したデジタルレコーダ１０を含む。このデジタルレコーダ１０は、衛星アンテナ、又は、ケーブルネットワークに接続され、サービスプロバイダによって配信ビデオ番組を受信する。これらの番組は、たとえば、ＭＰＥＧ２フォーマットの

データのストリームＦで受信される。公知の方法で、これらの番組は、スクランブルをかけられた形式で伝送され、そのコンテンツは、制御語ＣＷによってスクランブルされている。これらの制御語は、それ自体が、伝送中に秘密の状態を保ったまま所与の暗号アルゴリズムに従って鍵Ｋを用いて暗号化された形式で、データストリームＦ中で伝送される。

【００３４】

かくして、サービスプロバイダによって許可されたユーザだけが（たとえば、申込料金の対価として）伝送されたデータを復号化する権能を付与される。このため、プロバイダは、許可されたユーザに、制御語ＣＷを復号化するため役立つ鍵Ｋを供給する。殆どの場合に、番組を受信する権能は、ユーザが自分の申込料金を支払う間に限られた一時的な権能である。したがって、鍵Ｋは、サービスプロバイダによって定期的に変更される。

【００３５】

本発明によれば、以下に説明するように、ユーザは、自分が加入している間に伝送された番組を記録し、自分が加入者ではなくなった場合でも、自分のネットワーク上で希望の頻度で番組を再生することができる。これに対し、データは、暗号形式で記録されるので、そのデータを記録したユーザのネットワーク以外のネットワークでそのデータを再生することができない。

【００３６】

図１において、ネットワークの状態は、全ての装置が図２及び３を参照して後述する処理に応じて接続されている状態である。

【００３７】

次に、デコーダ１０によって受信されたストリームＦで伝送されたデータが処理される様子を説明する。当業者には公知のように、ＭＰＥＧ２フォーマットに従って伝送されたデータの場合、データストリームＦは、一連のビデオデータパケット、オーディオデータパケット、及び、管理データパケットを含む。管理データパケットは、特に、制御メッセージＥＣＭ（権利制御メッセージの略）を含む。制御メッセージＥＣＭでは、ビデオパケット及びオーディオパケットで伝送されたデータにスクランブルをかけるため利用される制御語ＣＷが、鍵Ｋを用い

た暗号形式で伝送される。

【００３８】

このデータストリームＦは、スマートカード１１へ送信され、スマートカード内で処理される。データストリームＦは、デマルチプレクサ回路（ＤＥＭＵＸ）１２によって受信され、デマルチプレクサ回路は、ＥＣＭをアクセス制御回路ＣＡ１３へ送信し、スクランブルをかけられたビデオデータ及びオーディオデータのパケットＤＥをマルチプレクシング回路（ＭＵＸ）１５へ送信する。回路ＣＡは、鍵Ｋを保持し、ＥＣＭに収容された制御語ＣＷを復号化することが可能である。回路ＣＡは、これらの制御語ＣＷを変換器回路１４へ送信する。本発明によれば、変換器回路１４は、ネットワークのローカル公開鍵$K_{PUB.LOC}$を保持する。変換器回路１４は、この鍵$K_{PUB.LOC}$を使用し、制御語ＣＷを暗号化し、ローカル公開鍵を使用して暗号化されたこれらの制御語を、制御メッセージＬＥＣＭでマルチプレクシング回路１５へ送信する。これらのメッセージＬＥＣＭは、初期データストリームＦで受信されたメッセージＥＣＭと同じ機能を備えているが、メッセージＬＥＣＭの場合に、制御語ＣＷは、サービスプロバイダの鍵Ｋを用いて暗号化されるのではなく、ローカル公開鍵$K_{PUB.LOC}$を用いて暗号化されている点が相違する。

【００３９】

マルチプレクシング回路１５は、データパケットＤＥと、変換された制御メッセージＬＥＣＭを、データストリームＦ’として送信し、データストリームＦ’はデコーダ１０によって受信される。家庭用バスＢのあちらこちらを流れるデータストリームは、このデータストリームＦ’であり、データストリームＦ’は、いずれか１台の提示装置２又は３によって受信され、或いは、デジタルビデオレコーダ４によって受信され、記録される。本発明によれば、データは、バスＢ内を常に暗号形式で流れ、ネットワークのローカル秘密鍵$K_{PRI.LOC}$を収容する装置だけが制御語ＣＷを復号化し、データＤＥを復号化し得る。したがって、これは、図１の家庭用ネットワークで作成された全てのコピーが他のローカルネットワークへブロードキャストされることを阻止される。

【００４０】

図１の例の場合に、回路１２乃至１５は、スマートカード１１と一体化してもよいが、他の変形例では、回路ＤＥＭＵＸ及び回路ＭＵＸはデコーダ１０に収容し、残りの回路１３及び回路１４がスマートカードに一体化される。とくに、回路ＣＡ１３及び変換器回路１４は、復号鍵及び暗号鍵を収容するので、これらの回路は、スマートカードのような安全な媒体に組み込まれる。

【００４１】

提示装置２は、スマートカード２１を搭載したスマートカードリーダを具備したデジタルテレビジョン受像機（ＤＴＶ１）２０を含む。受像機２０は、バスＢを介して、デコーダ１０、若しくは、デジタルビデオレコーダ４から発生されたデータストリームＦ’を受信する。データストリームＦ’は、スマートカード２１へ送信される。データストリームＦ’は、デマルチプレクサ回路（ＤＭＵＸ）２２で受信され、デマルチプレクサ回路（ＤＭＵＸ）２２は、スクランブルをかけられたビデオデータパケット及びオーディオデータパケットＤＥを、スクランブル解除回路（ＤＥＳ．）２４へ送信し、変換された制御メッセージＬＥＣＭを端末モジュール２３へ送信する。端末モジュールは、ネットワークの公開鍵（$K_{PUB.LOC}$）と秘密鍵（$K_{PRI.LOC}$）のペアを収容する。制御メッセージＬＥＣＭは、ネットワークのローカル公開鍵$K_{PUB.LOC}$を用いて暗号化された制御語ＣＷを収容するので、端末モジュールは、ネットワークのローカル公開鍵$K_{PUB.LOC}$を用いて、これらの制御語を復号化することができ、制御語ＣＷを平文で取得することができる。これらの制御語ＣＷは、スクランブル解除回路２４へ送信され、スクランブル解除回路２４は、データパケットＤＥのスクランブルを外すためこれらの制御語ＣＷを使用し、平文のデータパケットＤＣをテレビジョン受像機２０へ出力する。

【００４２】

平文データＤＣがスマートカード２１と、テレビジョン受像機２０のディスプレイ回路との間で最終的に伝送されることを確保するため、スマートカードと、受像機２０のカードリーダとの間のインタフェースＩは、スマートカードの安全性を確保するため、たとえば、米国ＮＲＳＳ標準（ナショナル・リニューワブル・セキュリティ・スタンダード）に準拠して作成される。

【００４３】

第２の提示装置３は、スマートカード３１が搭載されたスマートカードリーダを具備したデジタルテレビジョン受像機（ＤＴＶ２）３０を含み、第１の提示装置２と全く同様に動作するので、これ以上の説明を加えない。

【００４４】

上述のローカルデジタルネットワークを用いることにより、コンテンツプロバイダから生じたデータストリームＦは、データストリームＦを受信するアクセス装置によって、ネットワークのローカル公開鍵$K_{PUB.LOC}$を用いてデータストリームＦ’へ変換される。このデータストリームＦ’は、ローカルネットワークに特有のフォーマットを有し、このデータは、ローカルネットワークのローカル秘密鍵を保持するこのローカルネットワークの提示装置以外の装置では復号化し得ない。

【００４５】

次に、図１のローカルデジタルネットワークが作成される態様、及び、ネットワークの全ての装置がネットワークの固有のローカル鍵のペアを共用することを保証するように、新しい装置のこのローカルネットワークへの接続が管理される態様を説明する。

【００４６】

本発明によるデジタルネットワークを作成するため、アクセス装置と提示装置を一体的に接続する必要がある。

【００４７】

図２では、最初に、ネットワークは、デジタルバスＢを用いて、アクセス装置１と提示装置２を接続することにより作成される場合を考える。ネットワークを作成する処理の種々の手順は、二つの装置の間で行われるやり取りを示すような形で時間軸ｔに沿って表わされている。

【００４８】

この処理の第１のステップ１００において、２台の装置が一つに接続されたとき、提示装置は、公開鍵K_{PUB2}と秘密鍵K_{PRI2}のペアを収容し、本発明によれば、バージン状態にある。

【００４９】

装置の状態は、好ましくは、提示装置の端末モジュール２３（図１）に設けられた２ビットのレジスタである状態インジケータＩＥによって記憶される。慣例的に、装置がバージン状態であるとき、状態インジケータＩＥは００に一致し、装置が親状態であるとき、ＩＥ＝０１であり、装置が無効状態であるとき、ＩＥ＝１０であるとする。

【００５０】

状態インジケータＩＥは、耐タンパー性が保証されるように、スマートカード内の集積回路に収容される。

【００５１】

提示装置が製造元によって販売されたとき、本発明のタイプの既設のローカルネットワークに接続可能でなければならない。また、提示装置は、新しいネットワークを作成するようにアクセス装置へ接続可能でなければならない。そのため、本発明に従って製造された提示装置は、提示装置毎に固有であり、他の提示装置のものとは異なる公開鍵と秘密鍵のペアを必ず保持し、これにより、本発明に従って作成された各ローカルネットワークが、ユニークな鍵のペアを保持することを保証する。さらに、やり取りの機密性を保証するため、使用される全ての秘密鍵／公開鍵のペアは、当業者に公知の方法に応じて照明される。

【００５２】

アクセス装置は、暗号鍵／復号鍵を保持しない状態で製造、販売される。アクセス装置は、好ましくは、図１に関して説明したように、本発明による（スマートカードに収容された）変換器回路を含み、接続されるネットワークのローカル鍵を記憶することができる。

【００５３】

図２を参照するに、この処理のステップ１０１において、提示装置２は、バス２を介して、バスＢに接続される資格のある全てのアクセス装置、本例では、アクセス装置１を宛先として公開鍵K_{PUB2}を配布する。

【００５４】

ステップ１０２において、アクセス装置１は、公開鍵K_{PUB2}を受信し、ネ

ットワークの新しいローカル公開鍵（$K_{PUB.LOC}=K_{PUB2}$）として記憶する。

【００５５】

ステップ１０３において、アクセス装置１は、バスＢを介して、提示装置２を宛先として、状態変更信号を配布する。このステップは、最初にネットワークへ接続すべきこと、並びに、ネットワークの親になるべきことを提示装置２に報せることを目的とする。換言すると、この提示装置２が秘密鍵K_{PRI2}をネットワークへ接続されるべき新しい提示装置へ送信することが許可された唯一の提示装置である旨を提示装置２へ報せる。

【００５６】

ステップ１０４において、提示装置２は、状態変更信号を受信し、親状態（ＩＥ＝０１）へ移るように状態インジケータを変更する。

【００５７】

この処理の最後に、ネットワーク中の装置に公開された（提示装置２の初期公開鍵K_{PUB2}と等しい）固有のローカル公開鍵$K_{PUB.LOC}$と、提示装置２だけが知っている固有のローカル秘密鍵$K_{PRI.LOC}$を有する本発明によるローカルデジタルネットワークが得られる。ネットワークは、本は詰めによれば、新しい提示装置の接続を許可することによりネットワークを変更することができる親提示装置を含む。

【００５８】

次に、図３を参照して、本例の場合に提示装置３である新しい提示装置を、図２の処理に従って作成されたネットワークへ接続する処理を説明する。

【００５９】

この処理の最初のステップ２００、２００’及び２００”において、提示装置３を、デジタルバスＢを介して、既存のローカルネットワークへ接続する。提示装置３は、固有の公開鍵K_{PUB3}と秘密鍵K_{PRI3}のペアを収容し、バージン状態（ＩＥ＝００）である。アクセス装置１及び提示装置２は、図２の処理の最後の状態と同じ状態であり、アクセス装置１は、ネットワークのローカル公開鍵$K_{PUB.LOC}$を保持し、提示装置は、ネットワークの親状態（ＩＥ＝０１

）であり、ネットワークのローカル鍵のペア$K_{PUB.Loc}$及び$K_{PRI.Loc}$を保持する。

【００６０】

第２のステップ２０１において、提示装置３は、バスＢを介して、バスＢへ接続する資格のある全てのアクセス装置、本例の場合には、アクセス装置１へ向けられた公開鍵K_{PUB3}を配布する。このステップは、作成処理のステップ１０１（図２）と同じステップである。

【００６１】

ステップ２０２において、アクセス装置１は、公開鍵K_{PUB3}を受信し、アクセス装置１が既に公開鍵を保持しているかどうかを照合する。

【００６２】

本例のように照合結果が肯定的である場合、次のステップ２０３において、アクセス装置１は、バスＢを介して、新しい提示装置３へ向けてローカル公開鍵$K_{PUB.Loc}$を配布する。

【００６３】

ステップ２０４において、提示装置３は、ローカル公開鍵$K_{PUB.Loc}$を受信し、そのローカル公開鍵を好ましくは端末モジュールに記憶する。

【００６４】

ステップ２０５において、提示装置３は、バスＢを介して、ネットワークの全ての提示装置へ、ネットワークの親装置が応答することを要求するメッセージの形式（Ｇｅｎｉｔｏｒ？）で信号を配布する。

【００６５】

ステップ２０６において、ネットワークの親装置、本例の場合に、提示装置２は、このメッセージを受信し、提示装置２と提示装置３の間で信頼できる形で通信が確立された後、提示装置２は、無効状態（ＩＥ＝１０）へ移るように状態を変更する。

【００６６】

ステップ２０７において、提示装置２は、ネットワークのローカル秘密鍵を、提示装置３によって復号化可能な暗号形式（$E(K_{PRI.Loc})$）で配布す

る。特に、提示装置２と提示装置３の間におけるこのローカル秘密鍵の安全な伝送は、ローカル秘密鍵を暗号化するための提示装置３の初期公開鍵K_{PUB3}を用いて行われ、提示装置３は、この秘密鍵K_{PRI3}を用いてこのメッセージを復号化することができる。鍵K_{PUB3}は、たとえば、ステップ２０５の間に提示装置２へ送信される。

【００６７】

ステップ２０８において、提示装置３は、このローカル秘密鍵を受信し、好ましくは、スマートカード３１（図１）と一体化された端末モジュールへ記憶させる。

【００６８】

ステップ２０９において、提示装置３は、ローカル秘密鍵の受信を承認する信号を、バスＢを介して提示装置２へ配布する。

【００６９】

ステップ２１０において、提示装置２は、この受信承認信号を受信し、これに応答して、状態変更信号を新しい提示装置３へ配布し、ステップ２１１において、提示装置３は、この信号を受信し、ネットワークの新しい親になるように状態を変更する（ＩＥ＝０１）。

【００７０】

提示装置２は、これ以降、無効状態になるので、ネットワークのローカル公開鍵を他の提示装置へ送信することが許可されなくなる。これにより、上述のネットワークと同じローカル鍵のペアを保有する別の不正なローカルネットワークを作成するため、この装置２をネットワークから取り除くことが阻止できるようになる。

【００７１】

この処理の最後に、２台の提示装置２及び３と１台のアクセス装置１とが、ローカルネットワークに接続されている。これらは、ネットワークのローカル鍵のペア$K_{PUB.LOC}$及び$K_{PRI.LOC}$を共用する。ネットワークには、常に、ネットワークに最後に接続された提示装置、すなわち、固有の親装置が存在する。

【００７２】

本発明によるアクセス装置が鍵を備えることなく販売されるので、新しいアクセス装置のローカルネットワークへの接続は、非常に簡単である。特に、新しいアクセス装置がネットワークにプラグインされたとき、新しいアクセス装置が、バスＢを介して、ネットワークの公開鍵を受信することを要求するメッセージを配布するよう構成することが可能である。このメッセージを受信する第１のネットワーク装置、或いは、親装置だけが、このメッセージに応答して、ネットワークの公開鍵を新しいアクセス装置へ配布するよう構成することが可能である。

【図面の簡単な説明】

【図１】

本発明によるローカルデジタルネットワークの説明図である。

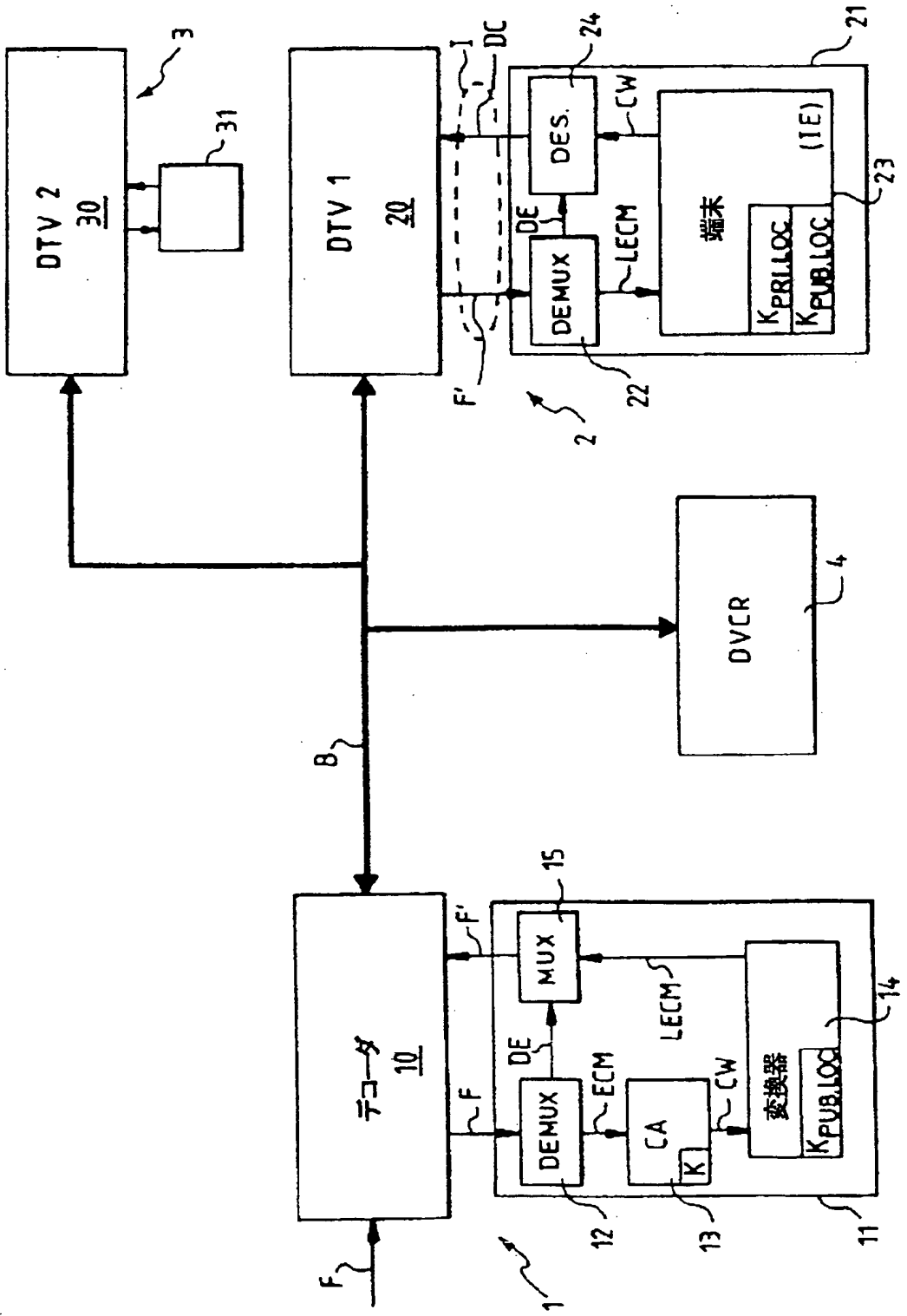
【図２】

図１に示されたローカルデジタルネットワークのようなデジタルネットワークを作成する方法の説明図である。

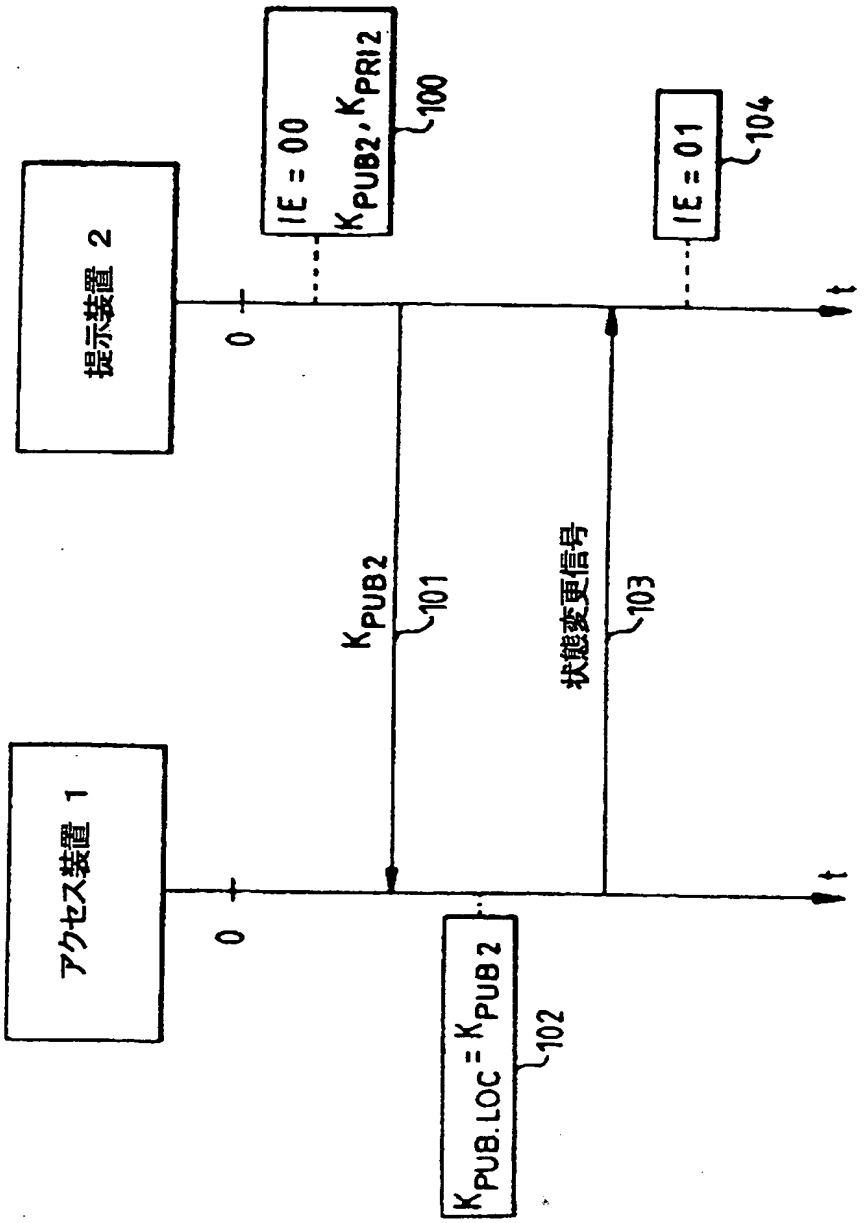
【図３】

新しい提示装置を、たとえば、図２に示された方法に従って作成されたローカルデジタルネットワークへ接続する方法の説明図である。

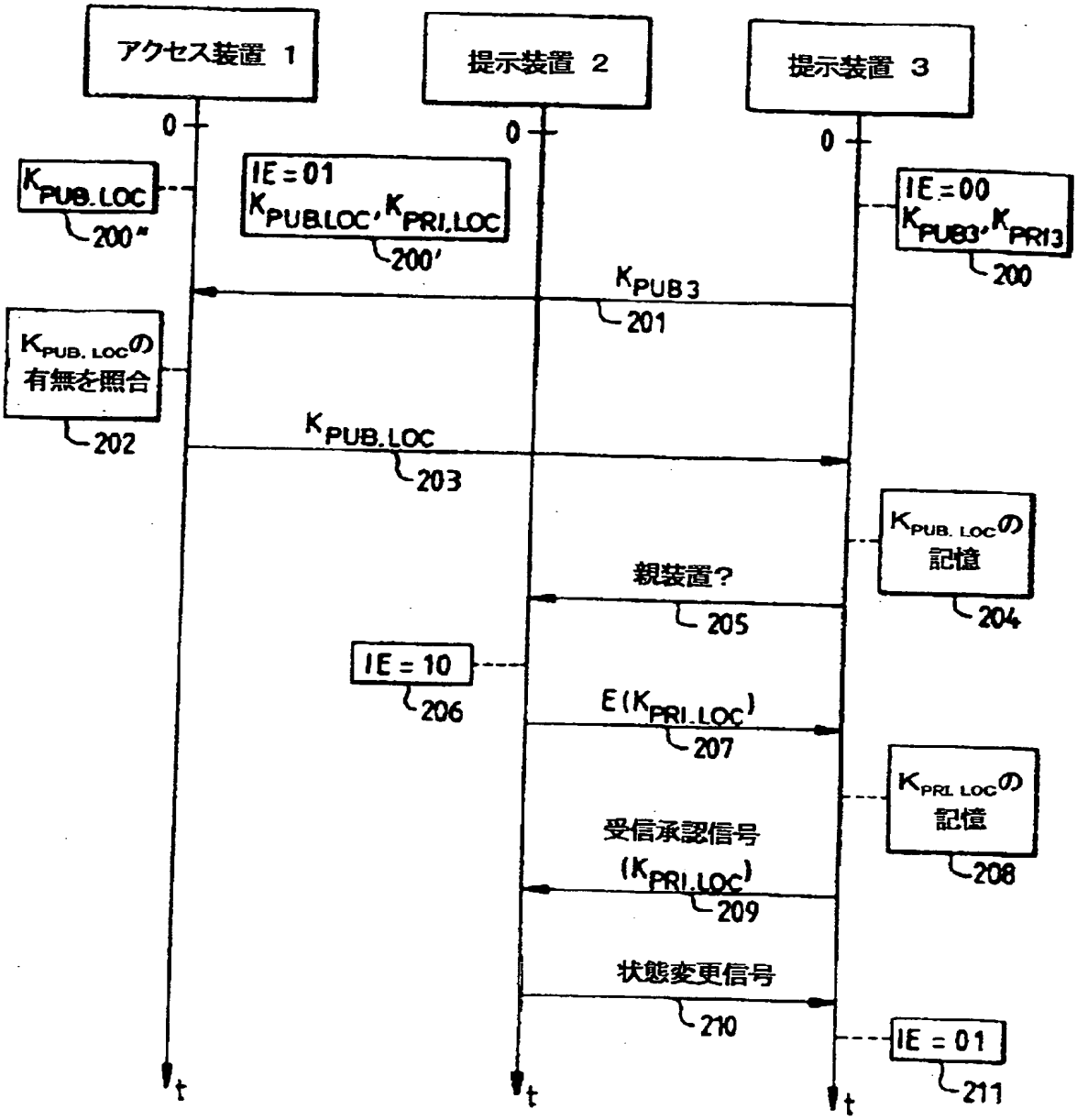
【図１】


DTV 2
30
3
31
DTV 1
20
DC
1
24
21
DES.
CW
DE
DEMUX
LECM
端末
(IE)
23
K_{PRIVOC}
K_{PUBLOC}
F'
22
2
DVCR
4
B
デコーダ
10
F
15
MUX
DE
DEMUX
ECM
CA
K
CW
LECM
変換器
14
K_{PUBLOC}
12
13
11
1
F

【図２】


提示装置 2
アクセス装置 1
0
0
t
t
IE = 00
K_{PUB2}, K_{PRI2}
100
IE = 01
104
K_{PUB2}
101
状態変更信号
103
$K_{PUB.LOC} = K_{PUB2}$
102

【図３】


アクセス装置 1
提示装置 2
提示装置 3
0
0
0
$K_{PUB.LOC}$
200"
IE=01
$K_{PUB.LOC}$, $K_{PRI.LOC}$
200'
IE=00
K_{PUB3}, K_{PRI3}
200
K_{PUB3}
201
$K_{PUB.LOC}$の有無を照合
202
$K_{PUB.LOC}$
203
$K_{PUB.LOC}$の記憶
204
親装置?
205
IE=10
206
E($K_{PRI.LOC}$)
207
$K_{PRI.LOC}$の記憶
208
受信承認信号
($K_{PRI.LOC}$)
209
状態変更信号
210
IE=01
211
t
t
t

【国際調査報告】

INTERNATIONAL SEARCH REPORT

Inte rnal Application No
PCT/EP 00/02918

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L29/06 H04L12/28

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 H04L H04N

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC, IBM-TDB, COMPENDEX

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 382 296 A (N.V. PHILIPS GLOEILAMPENFABRIEKEN) 16 August 1990 (1990-08-16)	1
A	column 2, line 2-37 column 3, line 12-29 column 4, line 40-44 column 4, line 55 -column 5, line 34 column 6, line 57 -column 7, line 5 column 8, line 56 -column 9, line 42	2-14
A	EP 0 679 029 A (SCIENTIFIC ATLANTA) 25 October 1995 (1995-10-25) page 2, line 22-41 page 3, line 31-34 page 3, line 47-50 page 7, line 34-57 page 9, line 46-57	1-14

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2000	21/07/2000

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Lázaro Lõpez, M.L.

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter nal Application No
PCT/EP 00/02918

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP 382296 A	16-08-1990	NL	8900307 A	03-09-1990
		AU	620298 B	13-02-1992
		AU	4911190 A	16-08-1990
		CA	2009290 A	08-08-1990
		CN	1045317 A,B	12-09-1990
		DE	69011543 D	22-09-1994
		DE	69011543 T	02-03-1995
		JP	2250439 A	08-10-1990
		KR	155373 B	16-11-1998
		US	4980912 A	25-12-1990
		US	5144662 A	01-09-1992
EP 0679029 A	25-10-1995	US	5237610 A	17-08-1993
		EP	0683614 A	22-11-1995
		AT	144670 T	15-11-1996
		AT	181196 T	15-06-1999
		AT	180373 T	15-06-1999
		AU	650958 B	07-07-1994
		AU	1384092 A	01-10-1992
		BR	9201106 A	24-11-1992
		CN	1066950 A,B	09-12-1992
		DE	69214698 D	28-11-1996
		DE	69214698 T	06-03-1997
		DE	69229235 D	24-06-1999
		DE	69229235 T	23-09-1999
		DE	69229408 D	15-07-1999
		DE	69229408 T	11-11-1999
		EP	0506435 A	30-09-1992
		JP	5145923 A	11-06-1993
		SG	44801 A	19-12-1997

フロントページの続き

(51)Int.Cl.[7]	識別記号	FI	テーマコード(参考)
G09C 1/00	660	G06K 19/00	Q
		H04L 9/00	601F

(81)指定国　EP(AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OA(BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), AP(GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), EA(AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW

(72)発明者　アンドル，ジャンーピエール
フランス国，35000　レンヌ，リュ・ド・ロンジェニル　20

(72)発明者　フュロン，テディ
フランス国，35000　レンヌ，リュ・ド・ラ・サンテ　13

Fターム(参考)　5B017 AA06 BA07 CA16
5B035 AA13 BB09 BC03 CA11
5B085 AE29 BC00
5J104 AA01 AA13 JA21 NA02 PA07